Security Vulnerability Assessment in accordance with the schedule provided in § 27.210.

(2) Notwithstanding paragraph (d)(1) of this section, a covered facility must update, revise, or otherwise alter its Security Vulnerability Assessment to account for new or differing modes of potential terrorist attack or for other security-related reasons, if requested by the Executive Assistant Director.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41891, Aug. 4, 2021]

§ 27.220 Tiering.

(a) *Preliminary determination of risk-based tiering.* Based on the information the Department receives in accordance with §§ 27.200 and 27.205 (including information submitted through the Top-Screen process) and following its initial determination in § 27.205(a) that a facility presents a high level of security risk, the Department shall notify a facility of the Department's preliminary determination of the facility's placement in a risk-based tier.

(b) *Confirmation or alteration of risk-based tiering.* Following review of a covered facility's Security Vulnerability Assessment, the Executive Assistant Director shall notify the covered facility of its final placement within a risk-based tier, or for covered facilities previously notified of a preliminary tiering, confirm or alter such tiering.

(c) The Department shall place covered facilities in one of four risk-based tiers, ranging from highest risk facilities in Tier 1 to lowest risk facilities in Tier 4.

(d) The Executive Assistant Director may provide the facility with guidance regarding the risk-based performance standards and any other necessary guidance materials applicable to its assigned tier.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41892, Aug. 4, 2021]

§ 27.225 Site security plans.

(a) The Site Security Plan must meet the following standards:

(1) Address each vulnerability identified in the facility's Security Vulnerability Assessment, and identify and describe the security measures to address each such vulnerability;

(2) Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water-borne explosive devices, ground assault, or other modes or potential modes identified by the Department;

(3) Identify and describe how security measures selected and utilized by the facility will meet or exceed each applicable performance standard for the appropriate risk-based tier for the facility; and

(4) Specify other information the Executive Assistant Director deems necessary regarding chemical facility security.

(b) Except as provided in § 27.235, a covered facility must complete the Site Security Plan through the CSAT process, or through any other methodology or process identified or issued by the Executive Assistant Director.

(c) Covered facilities must submit a Site Security Plan to the Department in accordance with the schedule provided in § 27.210.

(d) *Updates and revisions.* (1) When a covered facility updates, revises, or otherwise alters its Security Vulnerability Assessment pursuant to § 27.215(d), the covered facility shall make corresponding changes to its Site Security Plan.

(2) A covered facility must also update and revise its Site Security Plan in accordance with the schedule in § 27.210.

(e) A covered facility must conduct an annual audit of its compliance with its Site Security Plan.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41892, Aug. 4, 2021]

§ 27.230 Risk-based performance standards.

(a) Covered facilities must satisfy the performance standards identified in this section. The Executive Assistant Director will issue guidance on the application of these standards to risk-based tiers of covered facilities, and the acceptable layering of measures used to meet these standards will vary by risk-based tier. Each covered facility must select, develop in their Site

Security Plan, and implement appropriately risk-based measures designed to satisfy the following performance standards:

(1) *Restrict area perimeter.* Secure and monitor the perimeter of the facility;

(2) *Secure site assets.* Secure and monitor restricted areas or potentially critical targets within the facility;

(3) *Screen and control access.* Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,

(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and

(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;

(4) *Deter, detect, and delay.* Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;

(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;

(iii) Detect attacks at early stages, through countersurveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and

(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning;

(5) *Shipping, receipt, and storage.* Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;

(6) *Theft and diversion.* Deter theft or diversion of potentially dangerous chemicals;

(7) *Sabotage.* Deter insider sabotage;

(8) *Cyber.* Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems;

(9) *Response.* Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;

(10) *Monitoring.* Maintain effective monitoring, communications and warning systems, including,

(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;

(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

(11) *Training.* Ensure proper security training, exercises, and drills of facility personnel;

(12) *Personnel surety.* Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,

(i) Measures designed to verify and validate identity;

(ii) Measures designed to check criminal history;

(iii) Measures designed to verify and validate legal authorization to work; and

(iv) Measures designed to identify people with terrorist ties;

(13) *Elevated threats.* Escalate the level of protective measures for periods of elevated threat;

(14) *Specific threats, vulnerabilities, or risks.* Address specific threats, vulnerabilities or risks identified by the Executive Assistant Director for the particular facility at issue;

(15) *Reporting of significant security incidents.* Report significant security incidents to the Department and to local law enforcement officials;

(16) *Significant security incidents and suspicious activities.* Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;

(17) *Officials and organization.* Establish official(s) and an organization responsible for security and for compliance with these standards;

(18) *Records.* Maintain appropriate records; and

(19) Address any additional performance standards the Executive Assistant Director may specify.

(b) [Reserved]

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41892, Aug. 4, 2021]

§ 27.235 Alternative security program.

(a) Covered facilities may submit an Alternative Security Program (ASP) pursuant to the requirements of this section. The Executive Assistant Director may approve an ASP, in whole, in part, or subject to revisions or supplements, upon a determination that the ASP meets the requirements of this part and provides for an equivalent level of security to that established by this part.

(1) A Tier 4 facility may submit an ASP in lieu of a Security Vulnerability Assessment, Site Security Plan, or both.

(2) Tier 1, Tier 2, or Tier 3 facilities may submit an ASP in lieu of a Site Security Plan. Tier 1, Tier 2, and Tier 3 facilities may not submit an ASP in lieu of a Security Vulnerability Assessment.

(b) The Department will provide notice to a covered facility about the approval or disapproval, in whole or in part, of an ASP, using the procedure specified in § 27.240 if the ASP is intended to take the place of a Security Vulnerability Assessment or using the procedure specified in § 27.245 if the ASP is intended to take the place of a Site Security Plan.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41892, Aug. 4, 2021]

§ 27.240 Review and approval of security vulnerability assessments.

(a) *Review and approval.* The Department will review and approve in writing all Security Vulnerability Assessments that satisfy the requirements of § 27.215, including ASPs submitted pursuant to § 27.235.

(b) If a Security Vulnerability Assessment does not satisfy the requirements of § 27.215, the Department will provide the facility with a written notification that includes a clear explanation of deficiencies in the Security Vulnerability Assessment. The facility shall then enter further consultations with the Department and resubmit a sufficient Security Vulnerability Assessment by the time specified in the written notification provided by the Department under this section. If the resubmitted Security Vulnerability Assessment does not satisfy the requirements of § 27.215, the Department will provide the facility with written notification (including a clear explanation of deficiencies in the Security Vulnerability Assessment) of the Department's disapproval of the Security Vulnerability Assessment.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41892, Aug. 4, 2021]

§ 27.245 Review and approval of site security plans.

(a) *Review and approval.* (1) The Department will review, and either approve or disapprove, all Site Security Plans that satisfy the requirements of § 27.225, including ASPs submitted pursuant to § 27.235.

(i) The Department will review Site Security Plans through a two-step process. Upon receipt of the Site Security Plan from the covered facility, the Department will review the documentation and make a preliminary determination as to whether it satisfies the requirements of § 27.225. If the Department finds that the requirements are satisfied, the Department will issue a Letter of Authorization to the covered facility.